IEEE P802.11
Wireless LANs

|  |
| --- |
| Issues Tracking |
| Date: 2022-03-09 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W. Java DrSunnyvale, CA | +1 303 818 8472 | mark.hamilton2152@gmail.com  |
| AbstractIssues Tracking sheet for P802.11bh - Operation with Randomized and Changing MAC Addresses.…R14 – Added comments from August 9 telecon, including noting some specific “Action”s needed. A few suggested editorial changes.R15 – As updated during Sept 17 telecon (802.11 interim session)R16 – Editorial clean-up. Remaining items need technical review and agreement.R17 – Added references to proposed solutions in clause 6. Added summary tables in sections 5 and 6.R18 – Added alternative analysis approach in clause 6 (for TG discussion, which is more appropriate (or both)?R19 – As updated on Oct 26, 2021 teleconference. (Editorial alignment still needed)R20 – Editorial cleanup of Oct 26 changes/comments.R21 – As edited on Nov 4 teleconference, in section 6.R22 – Added rows to Table 2, based on Nov 4 teleconference. Updated references to proposed solutions.R23 – Updated on Nov 11 teleconf: reviewing summary table at top of clause 5, trying to confirm if we have agreement/consensus on use cases to consider and how to consider them.R24 – Upon review of Section 5, updates to use case 4.2 description, many notes on scope/requirementsR25 – Added note about different network security types, in 4.2.R26 – Updates per continued review of Section 5. R27 – Updates on Dec 16 telecon; completed review of Section 5, and therefore Section 6 criteria list.R28 – Clarified “post-association” to be clear this is after both association and security context.R29 – Updated tables 1 and 2 (Section 6) to match Section 5 discussion and agreements. Also, to be more useful as templates for separate solution analysis contributions.R30 – Updated proposed solutions references in section 6.R31 – Comment on use case 4.8 and added two use cases 4.27 & 4.28  |  |  |  |  |

**Table of Contents**

[1 Introduction 4](#_Toc95998118)

[2 Terminology 4](#_Toc95998119)

[3 Brainstorming ideas/discussion 5](#_Toc95998120)

[4 Use cases – “user level” view of behaviors and the gap between desired and current behaviors when RCM is used 5](#_Toc95998121)

[4.1 Pre-association client steering (AP steering, band steering, network steering) 5](#_Toc95998122)

[4.2 Post-association access control (Parental controls, etc.) 6](#_Toc95998123)

[4.3 Post-association home automation (including arrival detection) 6](#_Toc95998124)

[4.4 Airport Security Queue 6](#_Toc95998125)

[4.5 Grocery store customer flow analysis 7](#_Toc95998126)

[4.6 Grocery store frequent shopper notifications 7](#_Toc95998127)

[4.7 Infrastructure (home or enterprise) with different SSIDs per band 7](#_Toc95998128)

[4.8 Infrastructure (home or enterprise): Probes are randomized, even to/heard by associated AP 8](#_Toc95998129)

[4.9 Unapproved client detection in secured infrastructure network 8](#_Toc95998130)

[4.10 Approved client detection in secured infrastructure network 9](#_Toc95998131)

[4.11 Approved client in secured infrastructure network taking unsecured action 9](#_Toc95998132)

[4.12 Unapproved APs 9](#_Toc95998133)

[4.13 Mobile AP 9](#_Toc95998134)

[4.14 Onboarding a “known” MAC address (secure environment, or controlled/managed), but does anyone know the address? 9](#_Toc95998135)

[4.15 Customer Support and Troubleshooting 10](#_Toc95998136)

[4.16 Residential Wireless Gateway with Hotspot 10](#_Toc95998137)

[4.17 Lawful surveillance 11](#_Toc95998138)

[4.18 Emergency services (pre- or post-association) 11](#_Toc95998139)

[4.19 Public Wi-Fi hotspot and roaming (AP to AP – is this the same ESS??) 11](#_Toc95998140)

[4.20 MAC address collisions (WBA) 12](#_Toc95998141)

[4.21 Accounting and billing issues (WBA) 12](#_Toc95998142)

[4.22 QoS and QoE (WBA) 12](#_Toc95998143)

[4.23 DHCP pool exhaustion (WBA) 13](#_Toc95998144)

[4.24 Inconsistent DHCP address assignment (WBA) 13](#_Toc95998145)

[4.25 ACLs/firewalls (IP-address based ACL?) (WBA) 13](#_Toc95998146)

[4.26 Virtual BSSID (follow the user) 13](#_Toc95998147)

[5 Issues and analyses – discussion of 802.11 features/actions, per se 14](#_Toc95998148)

[6 Proposed Solutions 15](#_Toc95998149)

[6.1 Signature-based method for identifying STAs 15](#_Toc95998150)

[6.2 Identifiable random MAC address 15](#_Toc95998151)

[6.3 Client ID query 16](#_Toc95998152)

[6.4 Transient STA ID 16](#_Toc95998153)

[6.5 Secure Device ID exchange 16](#_Toc95998154)

[6.6 Opaque Device ID 16](#_Toc95998155)

[6.7 STA Generated Device ID 16](#_Toc95998156)

[6.8 MAC Address Designation (MAAD) 16](#_Toc95998157)

[6.9 Network Generated Device ID 16](#_Toc95998158)

[6.10 Solutions analysis 16](#_Toc95998159)

# Introduction

This document serves as a tracking sheet for issues raised within the context of P802.11bh, Operation with Randomized and Changing MAC Addresses.

Section 3 is a “scratch pad” for brainstorming comments and ideas, and other discussion points to remember.

Section 4 has a set of use cases which provide real-world example contexts in which some issue(s) arise from randomized and/or changing MAC addresses. These include use cases that have been identified for which we believe either the solution is outside our scope, or the solution already exists, and we will so comment on the use case. (That is, the use cases list includes all the use cases that the task group has considered, even when the conclusion is that no changes are needed/appropriate in IEEE Std 802.11.)

Specific technical issue are then presented in Section 5, including a technical description of the scenario which raises the issue (and mapping back to relevant use case(s)), the technical details of the problem, and the impacts on the overall system including what users/components are impacted, what 802.11 features are

Section 6 provides proposed technical solutions to address the issues (including mapping back to the specific issue(s) addressed by each solution), and discussion of any trade-offs or shortcomings of the solution.

# Terminology

**Randomized MAC address:** An individual MAC address (layer-2 MAC/PHY entity identification, or more specifically a MAC SAP identification) used by a MAC entity as its identification, but that is either not assigned as a globally unique or is not a permanent identifier (in what scope?).

NOTE: Such randomized MAC address should have the U/L bit set to indicate a local MAC addresses, per Std IEEE 802-2014. For the scope of this document, no compliance with 802c-2017 or P802.1CQ direction is assumed.

NOTE: The duration of use of the randomized address could be permanent or only for a shorter duration. Such a randomized address can obscure the real identification of the device and/or its user, for purposes of privacy, for example.

Syn: Local MAC address (OR… do we say it is a special case of Local MAC address, and say something about how it is special?)

Something about 802c-2017??

When dot11MACPrivacyActivated??

P802.1CQ??

**Changing MAC address**: A MAC address which is also changed over time. Such changes may be periodic, event driven, or triggered by other inputs. Note that IEEE 802.11 requires that a device’s MAC address not change during the lifetime of an association to an ESS. However, the time bounds of such an ESS association are not clearly specified or signalled in 802.11, and the interpretation of this requirement is varying across implementations.

**Rapidly changing MAC address**: A Changing MAC address which is generally changed within a time-frame that is approximately equal or less than the time constants for an 802.11 feature, usually impacting the feature’s correct operation.

NOTE—the interval that defines whether a changing MAC is rapidly changing varies with the feature and use case being considered, but is generally on the order of several minutes or less. For instance, changing MAC address in each probe request, or changing MAC address between each new association to the same ESS.

# Brainstorming ideas/discussion

* Lawful intercept requirements and/or limitations
* Use cases where privacy is desired/expected
	+ Privacy from whom?
	+ Privacy of what information? MAC address, and/or other information. How is the information used?
	+ User consent?
* Use cases where RCM is causing issues
* Pre-association and/or post-association (to the ESS) use cases
* Network operator monitoring location of assets
* Duplicate MAC addresses and issues caused
* STA “doesn’t want to/care about maintaining state” with the network
* What does it mean (or multiple meanings) for “opt-in”
* What is the limit of our PAR scope on privacy concerns being created?
* TGaz ranging, pre-association or post-association, TGaz’s security?
* TGbc features (pre-association/non-associated)

# Use cases – “user level” view of behaviors and the gap between desired and current behaviors when RCM is used

## Pre-association client steering (AP steering, band steering, network steering)

The user brings a phone within range of a multiple-AP infrastructure. Before connecting to the 802.11 network, the phone scans to discover the available APs, by sending Probe Requests, ANQP or other public action frames, etc.

* Use case splits: previously visited network might imply re-use of the same MAC address, or there might be a feature to change MAC address anyway
* Use case splits: device might have an SLA “agreement” with a previously visited network
* Use case splits: Device is probing specific SSID, or Broadcast SSID

During this scanning, (assuming the infrastructure has multiple APs, which includes a single AP device that is multi-band) the infrastructure monitors the signal levels received from the smartphone at multiple APs and bands on those APs, determines which AP and band will provide the best service, and steers the client to that AP. This saves the client power by directing its scans to shorten its scan and AP selection procedure and avoiding requiring it to scan all supported channels and bands, and also saves the infrastructure from needing to steer the client after attachment which saves time, connection disruption and bandwidth for management frames.

## Post-association access control (Parental controls, etc.)

NOTE: “Post-association” means after both association is complete, and security context is established.

People want all their devices to be recognized when attaching to the 802.11 network and control access to Internet content based on the user of various devices, without launching an application or using a portal. And, this needs to use a method that isn’t easily hacked and circumvented. For a visiting device, the device should be given only very limited access (if any at all) to the 802.11 network and Internet; thus unknown devices need to be distinguishable from one of the approved devices. For example, existing parental control offered in 802.11 routers is usually based on the MAC address of the device. Another example: pass/block list.

This scenario can be handled with a client-side “opt-in” method for providing a device or user identification that is hidden from third party snooping, and provided only to trusted infrastructure (for example, where RSN has been established). Any broader solution (not explicitly “opt-in”, not secured from snooping, or not restricted to trusted infrastructure) is considered out of scope for 802.11bh.

## Post-association home automation (including arrival detection)

NOTE: “Post-association” means after both association is complete, and security context is established.

Similarly, two trends in home automation are converging: use of 802.11 technologies as the ‘backbone’ of the automation system; and a feature of the automation system which allows it to recognize when one of the residents arrives and “welcoming” them home by turning on lights, music, etc., tailored to the individual. This convergence means that using the 802.11 network to detect the individual’s arrival, by detecting their personal 802.11 device (smartphone, etc.) is a highly desirable capability. Currently, this device recognition is usually done based on the MAC address.

Key point: the device (user) is voluntarily opting-in to this system. Also key that protection from third-party tracking is included.

This scenario can be handled with an “opt-in” method for providing a device or user identification that is hidden from third party snooping, and provided only to trusted infrastructure (for example, where RSN has been established). Any broader solution (not explicitly “opt-in”, not secured from snooping, or not restricted to trusted infrastructure) is considered out of scope for 802.11bh.

## Airport Security Queue

Airport security (and immigration) line wait times can reach times of an hour or more. It has become a feature of airports to offer information about lines’ wait times to passengers, which requires the ability for an automated system to measure the “average” time individuals are spending in these lines.

A common idea for such measurement is to “track” the 802.11 devices carried by people in the lines through their exposed MAC addresses, and detect how long the devices are, effectively, stationary in the area of the queue.

Such tracking generally needs to be effective on devices that are not connected to any network, especially, for example, in an airport where the 802.11 network is a fee-based service, so few people are attached. Further, the tracking needs to be effective across time spans of an hour or more for worst-case busy hours, when the information is most critically needed and needs to be accurate.

Upon analysis of this scenario, it has been agreed that such tracking of individuals without their consent is considered a violation of their privacy – exactly what MAC randomization is trying to prevent. Since the fundamental purpose of this tracking can be accomplished in other ways without 802.11 involvement, this scenario is considered out of scope for 802.11bh to provide a solution.

## Grocery store customer flow analysis

It is now common for a grocery store (or similar retail spaces) to do considerable analysis of the “traffic flow” of their customers. Doing this lets the store recognize the areas that are frequented by most/many customers and also the common pairings or patterns of multiple areas that are frequented in the same visit by many customers. This could be reasons that help the customer (putting frequent items near the front of the store, putting common combinations near each other), or that help the store despite the customer (putting frequent items or frequent combinations far apart, to force the customer to walk through the rest of the store), but either way, someone is benefiting and expects to be able to gather the information to implement their policy.

However, the store does not need to have any information about the actual identity of the people being tracked. Further, the store needs to track people that have no relationship with the store, and are not associating to the store’s network, e.g. through tracking the MAC address of public /non-associated frames from their 802.11 devices.

To discover useful patterns, the store needs to track individuals for a reasonable period of time – say, roughly a half hour at a minimum. At reasonable/lower cost.

Upon analysis of this scenario, it has been agreed that such tracking of individuals without their consent is considered a violation of their privacy – exactly what MAC randomization is trying to prevent. Since the fundamental purpose of this tracking can be accomplished in other ways without 802.11 involvement, this scenario is considered out of scope for 802.11bh to provide a solution.

## Grocery store frequent shopper notifications

A very different use case from the grocery store foot traffic analysis, is a grocery store that wants to recognize and reward frequent shoppers. This is likely to be an “opt-in” service, where the shoppers that are interested in participating with the store indicate that they are willing to have the store know some identity that the store can use (possibly not their true or complete identity, however). For maximum effectiveness, such programs need to recognize when the customer enters (or approaches) the store, and provide information (such as daily specials for frequent shoppers) without any action on the user’s part. Additionally, the store could be able to build a profile of the user, and push content (with a cellular text, perhaps, since the customer may not be associated to the store’s network) such as items that of likely interest to the customer and are on sale/special, when the customer is near those items in the store.

If this scenario is limited to opt-in uses, and it can be assumed that the device will have been configured to associate to the grocery store infrastructure when in range (and is associated), then the scenario can be handled with an “opt-in” method for providing a device or user identification that is hidden from third party snooping, and provided only to trusted infrastructure (for example, where RSN has been established).

Any broader solution (not explicitly “opt-in”, not secured from snooping, or not restricted to trusted infrastructure) is considered out of scope for 802.11bh.

## Infrastructure (home or enterprise) with different SSIDs per band

This use case is in reaction to two situations: first is a network where (for whatever reason, perhaps incorrectly) the network (a single LAN, under single network management, really) has been deployed with different SSIDs on different bands (“XYZ24G” and “XYZ5G”, for example); and second is considering a device that will use a consistent MAC address for a given SSID, but generates a new Local-ID MAC address for each new SSID. These scenarios have both been seen, relatively commonly, in the field.

In combination, these two scenarios result in the network infrastructure being unable to correlate the device’s signals, location, and network interaction on the two bands, which makes infrastructure band steering effectively impossible.

This scenario is considered out of scope for an 802.11bh solution. Deploying an intended single ESS with more than one SSID is beyond the scope or correct operation for 802.11. If a given single “network” (802 access domain) is deployed with multiple ESSs providing access, the device would not be able to maintain any shared state across the ESSs, unless it uses a consistent MAC address (see: 802.11aq). While a solution to indicate to the client that these ESSs are in fact a single network might be possible, it appears to be solving a problem caused by incorrect deployment, not by MAC address randomization.

## Infrastructure (home or enterprise): Probes are randomized, even to/heard by associated AP

A client that is using Local-ID MAC addresses could easily have an implementation that generates a new Local-ID MAC address for every Probe Request. This could even apply to Probe Requests that are directed to the associated SSID, when the client would otherwise use a consistent MAC address for transmissions within an association.

If the client has this extreme (or approaching this extreme) of an implementation of MAC address randomization, it will have a strong impact on the infrastructure’s ability to making steering decisions for that client.

When attached to a multiple-AP infrastructure, if the client uses the stable MAC address when probing, the infrastructure can help steer the client across both APs and bands, to give the entire network better experience. This could apply to both directed probes and broadcast probes, too.

Recommendations could be added to the Standard, to discuss the use of MAC addresses in scanning. There are trade-offs to be considered for a client to balance privacy and providing information to the network that could improve user experience.

It should also be noted that passive scanning is becoming more common, so reliance on identifiable probes for client steering has other problems, already.

## Unapproved client detection in secured infrastructure network

A managed WLAN network may desire to detect unapproved client stations operating in its service area, even when they do not (cannot) connect to the network.

In a (physically) controlled/secured environment, there is desire to know all the clients in the facility/area, and for the WIPS to detect this and alarm (perhaps based on ongoing probing without connecting).. With stable and globally unique MAC addresses, non-AP STAs could be listed on a known client list, by MAC address, and thereby unexpected/unwanted client devices in the service area can be detected, by detecting unknown MAC addresses. With RCM, this is no longer effective or practical.

In such an environment, physical controls over persons entering is needed (and used) already, so use case of unapproved devices in the area is not in our scope. Also, there’s no new problem here, due to RCM (couldn’t an attacker spoof a known client’s address, anyway?), so this problem is not in our scope to solve.

## Approved client detection in secured infrastructure network

For approved clients using RCM, this appears to be the same as other post-association cases, with the additional benefit that network security (802.1X) is likely in use and can address the device identification. What about controlling user behavior with their devices, even if there are physical controls?

What about an approved device before it associates/as it is probing? Will an RCM device use a “known” MAC address for probing a known SSID (only after detecting the SSID is present, just before associating)? Maybe, but not for broadcast probes. Approved devices may need a specific policy (when we get to solutions)?

## Approved client in secured infrastructure network taking unsecured action

It is desired to detect a known device that is suddenly taking unexpected/undesired actions, like attaching to a non-secure SSID. This use case is out of scope for TGbh. 802.11 does not support (or assume) an identifier that is shared across SSIDs.

## Unapproved APs

A managed WLAN network may desire to detect unapproved access points operating in its service area. One such unapproved AP detection mechanism entails monitoring for users associated to access points which are not known to be part of the managed network. The MAC addresses of the known APs are kept in a database, and the medium is monitored for Beacons or other broadcast traffic from, or non-AP STAs’ traffic to, APs not on the known AP list.

When an unapproved AP is detected, appropriate action (such as contacting the owner) can be taken to resolve any issues such as interference with the operation of the managed WLAN.

Off-the-shelf systems/solutions (that use Wi-Fi):

Not a use case affected by RCM. Might be another policy controlled situation, to retain MAC address.

## Mobile AP

Mobile AP detection in an enterprise (controlled environment) is beyond/not really an RCM problem, but some higher agreement problem with the user.

What about home use case? Note that mobile AP has a short lifetime.

A mobile AP will cause connectivity issues if the MAC address (==BSSID) changes. So, the mobile AP shall not change while clients are connected, and shall not change while beaconing. (Could add a recommendation to do tear down after a timeout if no clients are attached?) Between times when devices are connected (changing while no device is connected) is okay, because AP will use the same SSID when restarted, and clients do not need to discover the same BSSID.

Might make recommendations (or do we need to have a solution to this?); but note that 802.11 doesn’t have mobile AP (“soft AP”) concept (yet). Also, 802.11 does not have any spec text about an AP changing its address (11aq, etc., did not address this) – maybe add some guidelines?

## Onboarding a “known” MAC address (secure environment, or controlled/managed), but does anyone know the address?

Policy can handle secure environment. But, doesn’t solve onboarding.

Device count, of active devices (per credential), for BYOD environment. What about PSK/Passphrase networks (non-unique credentials)?

## Customer Support and Troubleshooting

Service providers are deploying wireless gateways in residential environments. With about two thirds of customer complaints related to WLAN, operators have to be able to provide top-notch technical support when a subscriber faces WLAN-related issues.

As an example, a subscriber has 16 devices connected to their 802.11 network. They have set-up different SSIDs for their guests, their kids, and their personal devices.  The subscriber is experiencing connectivity and low performance issue on their wireless network. Or, one of the devices in the residence is violating a policy, is detected by the ISP, and gets the entire residential service turned-off. When they call the technical customer center, the technician is able to identify the MAC address of the faulty device and ask the subscriber to reset its device and reconnect to the wireless network.

Broaden to cover enterprise case… In enterprise, can we rely on an authentication identification? (Machine versus user identification…) Pre-association (failure to associate) troubleshooting is still a problem.

Solution here may require help from device-based information/diagnostics.

Is this another “recommendations needed” situation?

<RCM makes the technician identifying a problematic device difficult.

RCM complicates identifying the device type from OUI.

Diagnosing actors: SP, AP vendor, WLAN admin.

Could ask user to turn off randomizing MAC. Could install a temporary app (if it has access to the “real HW MAC”). Need a SAP/MIB method to control the MAC doing randomization or reporting MAC address information outward/upward?>

## Residential Wireless Gateway with Hotspot

Service providers are deploying residential wireless gateways with public hotspots to expand their network coverage and capacity. With millions of hotspots available, subscribers can enjoy the benefit of complementary and seamless 802.11 connectivity while on the go. When a subscriber is at home, however, their devices should connect to the wireless home network rather than the hotspot available on the residential gateway. If a device connects to the hotspot, the subscriber doesn’t have access to their local network, cannot print files or access storage attached to the network. Neither can they enjoy their gigabit subscription. The gateway can prevent “home devices” from connecting to the hotspot based on their expected unique MAC address.

<Should the client device make this decision, connecting to the correct network? Or, should the public hotspot side of the gateway steer clients that connect to the “wrong” side? Agreed the client should handle this. Note that solutions for other use cases *might* happen to apply/help with this, but we will not target this use case. Perhaps not even a valid use case – we should not prevent clients from attaching to either network.

Bigger issue (beyond TGbh scope?) to do ESS steering of clients? >

## Lawful surveillance

Some organizations, both public and private, have a strong desire to monitor people in their behavior and habits. Having a device constantly emitting a unique identifier can help such these organizations surveil people. When people move around, sensors that passively detect these unique identifier emissions can make note of the identifier. Time and location of the sensor can combine with this datum to create a large database of information that can enable tracking of people. Habits can be recorded and observed and deviations from an established baseline can result in an alert regarding the person’s behavior. Artificial intelligence and big data analytics can use this database of information to facilitate this effort. A database of who is where and when can be used for a multitude of purposes, some lawful and some nefarious. Records in the database can be used as evidence in a government’s case against a citizen, and personal, and private information about people can be sold without their knowledge or approval.

802.11 is an obvious technology to build such a surveillance apparatus. Fixed MAC addresses will be used in mobile devices even when SIM cards are swapped out or removed. Laptops typically do not have a method of network access that is not bound to a MAC address. The tendency of unconnected devices to find a network results in active probing which can be passively detected, thereby enabling the surveillance apparatus. Indeed, the very nature of 802.11 network discovery and connection establishment compels exposure of MAC addresses and there is no way to disable their use. Using 802.11 to construct a surveillance database is an obvious choice.

<Privacy protection laws come into play. Governments, however, may sometimes override such laws (legally), to protect citizenry against criminals and terrorists for example. How do we support equipment that can comply with local regulations (both privacy, and legal tracking regulations) – but still protect privacy as required by our PAR? Balancing act, versus profiling, etc.

Opt-in or not (how this is different from a store/mall knowing a customer is present)? Document reference for legal intercept scenario? Are there legal intercept requirements for such tracking (or is it “if available”, not “compelled” – on the user, or on the provider)? IEEE 1609 might be an example, to help understand any requirement on 802.11.

Direction: we don’t believe we need to fix this use case; it would be good to have some evidence/support that we don’t have to fix it. “Happy accident” that this worked, ever – criminals know to not own/use such devices, anyway (?). This can be solved at another layer/another solution. Believe that any ‘fix’ would violate privacy, and therefore violate the PAR. We are not aware of any legal requirements that we solve this in the Standard.>

## Emergency services (pre- or post-association)

GAS and following association assumption of consistent MAC address, perhaps in scope. Emergency alerts are done via AP advertisement, not dependent on knowledge of clients. “E911” scenario to require location, and MAC address (not MAC, something else, like phone number, is used), of caller. NEAD has been cancelled. Future use of Wi-Fi location possibility, and does that create an issue? (This last sounds like new work, not 11bh scope to ‘fix’ something that broke.)

The GAS/association problem is probably just a bad assumption, and not something we need to fix. E911 seems to have no issues (see notes above).

## Public Wi-Fi hotspot and roaming (AP to AP – is this the same ESS??)

Non-AP STA: If this is a different ESS, you cannot Reassociate, so nothing is broken. (Same ESS is covered by 802.11aq requirement for stable MAC address.) PAR investigation …

Network side: Covered by use cases above.

## MAC address collisions (WBA)

< Add recommendation text “explaining how the 11aq language will/could/should work”: on number of bits to randomize (to help avoid the problem), use ANQP to get 802c policy for MAC addresses, and to take action to check for collisions? How to protect the ANQP/802c exchange (especially the policy to use your ‘true’ MAC)? >

## Accounting and billing issues (WBA)

MAC Address is tied to this in some use cases where rates rely on a unique device identifier. [This could be accomplished instead with proper support for Chargeable-User-Identity (CUI)].

Without MAC there may be diminished ability to handle Legal requirements for providing the type of information required for device traceability, device ownership, and legal intercept; but MAC was increasingly unreliable anyway.

< Two aspects:

1) Don’t understand how CUI can be used, as it is another temporary identifier.

2) Station identify itself to the network, in a protected manner, to (among other things?) select different billing charges.

Note that even before RCM, MAC addresses could be forged easily, so MAC address for billing really didn’t work, previously.

Move this use case from lower-left quadrant to lower-right quadrant? Need more details, to really do that (add to our reply liaison?). “It is that simple”: do the other A’s in AAA.

This is another example of use case 4.2 (we assume). >

## QoS and QoE (WBA)

QoS and QoE are popular features on which a lot of effort is being spent by Wi-Fi equipment vendors and Telecommunication equipment vendors in general.

QoS for example is important to allow prioritization for both services and devices in a network. It should be noted that a lot of the services and data connections consumed in residential networks are not properly QoS - tagged nor is it sometimes even possible to do so. For example, if a QoS rule would have to link with a device rather than an IP-based service.

Access points are as such configured with QoS/QoE rules to force Wi-Fi clients in a specific priority scheme such as a Wi-Fi Alliance® WMM access class or an AP’s airtime scheduling queue.

In In-Home Wi-Fi networks, Wi-Fi clients are identified by means of their unique MAC address, as such, the access points (APs) that form the network hold a synchronized list of MAC address to QoS/QoE mapping to ensure that Wi-Fi clients receive a uniform QoS/QoE treatment throughout the full network.

If Wi-Fi clients randomize their MAC address, they effectively remove themselves from the current QoS/QoE ruleset that has been put in place to improve their operation in the network.

< Trying to understand: Is this about multiple APs in a network, and continuing QoS treatment for a given client as it does AP-AP roaming? What about the 802.11 rule about a stable MAC address across AP-AP roaming? Could get clarification on this.

Do our SCS/mirrored SCS, etc., also come into this use case? What rules are being discussed?

Does protected means to identify device (use case 4.2) solve this? (If this is about a new association.) Robot going in and out of coverage example? >

## DHCP pool exhaustion (WBA)

MAC randomization has an impact on DHCP IPv4 address allocation. Devices asking for IP addresses or renewal are identified by MAC address and a device with a changed MAC will be seen as a different device. Where the IP lease time is longer than the lifetime of the randomized MAC address this can lead to IP pool exhaustion.

< Use short lifetime (lifetime < randomization interval) – might be user experience impacts. Or, if clients can/will, use a DHCP client identifier and address request to solve. Another alternative is the client identifier per use case 4.2. These would be recommendations on DHCP configuration/use. (note, this is exactly the sort of “state maintenance” that the 802.11aq text discussed).

How do we balance between a recommendation to use something like the DHCP identifier, versus 802.11 providing a mechanism for client identification? We should discuss. >

## Inconsistent DHCP address assignment (WBA)

MAC randomization has an impact on DHCP IPv4 address allocation. Devices asking for IP addresses or renewal are identified by MAC address and a device with a changed MAC will be seen as a different device. Devices that should have been allocated a fixed IP address will also not be identified as the owner of the IP address if they have randomized the MAC address.

(Use of client identifier and address request to solve?)

Same as the previous one, except short lifetime is not a solution here.

<Discuss ARP cache getting stale/needing to be flushed, also.>

## ACLs/firewalls (IP-address based ACL?) (WBA)

In any situation where the MAC address has been instrumental in providing an identifier for use in ACLs - the MAC itself, the IP Address, or a MAC-based hostname – then the ACL will not function as intended.

< This all sounds the same as use cases above (parental controls, etc.), except the IP address based variant.

What if there is something here that uses ACL for pre/at association behavior, a post-association and security context solution might not solve it. Also, if this is for security/ACL, is a device-provided identifier trusted sufficiently, or do we need to add authentication to that identifier? >

## Virtual BSSID (follow the user)

A given client device is “assigned” a generated BSSID. That BSSID moves from AP to AP within an ESS, to manage the client transitions.

Note: Device should not change its MAC address, while the association is held. So, no RCM problem here.

## STA Identification in Database

In some office environments, several APs are connected to each other. The administrator allocates an account (SSID/password) to a new user (e.g. new employee) to grant access to the network (e.g. company’s network) based on the cellphone’s MAC address. In such environment, (at least) one specific AP (as a controller that has an access to user database) should (1) be always turned on, (2) monitor the probe request frame from STA, so that the system can immediately turn on the corresponding AP for the relevant STA. If there are not many STAs in the network, the system will turn off some APs to save power and to reduce interference. This whole identification mechanism is based on STA MAC Address in database.

As an example, let’s consider a scenario, in which three APs co-exist (e.g. AP1 (SSID: Employee-1) as a controller, AP2 (SSID: Guest-1), and AP3 (SSID: Guest-2)). In this scenario, it is common that different APs provide different services. For instance, AP1 is an employee network (i.e. only employees can access), while AP2&3 are basic networks (e.g. just browsing websites). While an employee can get access to all APs (AP1, AP2, AP3) because of full authorization, a guest user can only get access to AP2 and AP3 because of limited authorization.

If an employee (STA1) associates with the network, AP1 saves the STA1 MAC (MAC1) in database. AP1 (as a controller) builds a communication link for STA1.

After STA1 leaves the network, AP1 turns off AP2 & AP3 to save power and reduce interference. AP1 (as a controller) remains active.

When STA1 comes with a new MAC (random MAC), i.e. MAC2, AP1 does not recognize MAC2. Therefore, AP1 cannot decide whether STA1 is an employee or not. Accordingly, STA1 is regarded as a guest and will not be allowed to access AP1 (employee network), even it is a real employee who should have an access to AP1.

Note that the similar issue can be applied to the residential environment as well.

## Deny/Allow List

“Allow/deny MAC address list” feature is widely used in current AP product, that is, (1) The administrator can disable some active STAs by adding their current MAC address to the deny list (AP rejects the auth/association request once the MAC address of requesting STA is in deny list) and/or (2) The administrator can enable some STAs by adding their current MAC address to the allow list (AP only allows the STA with the MAC address that is in the allow list.)

In this case, if a STA changes its MAC address (e.g. random MAC) each time it associates with AP, AP cannot recognize the STA’s identity, and cannot figure out its status in the allow/deny list.

For example, a STA (that is in deny list because of its MAC) still can associate with the AP through a new MAC because its new MAC is not in deny list in the system. In other words, that STA is granted access even though it should not be granted access. Similarly, a STA (that is in allow list with its MAC) can’t associate with the AP through a new MAC because its new MAC is not in allow list in the system. In other words, that STA is denied access even though it should be granted access.

# Issues and analyses – discussion of 802.11 features/actions, per se

The following table summarizes the use cases in clause 4, and their agreed applicability to 802.11 and 802.11 Working Group’s scope for changes to address those use cases.

|  |  |  |  |
| --- | --- | --- | --- |
| Use Case # | Use Case Name | Status | Agreement reached? |
| 4.1 | Pre-association client steering | “Nice to have” though, if can find sufficient privacy controls (opt-in, etc.) – maybe recommendation? Maybe if a solution to another problem happens to solve this? | Yes |
| 4.2 | Post-association ~~access control~~ (returning) device identification per network/SSID basis | In scope, (assuming we evaluate criteria): | Yes |
| 4.3 | Post-association home automation/arrival detection | In scope, (assuming we evaluate criteria): | Yes |
| 4.4 | Airport security queue | Out of scope to solve (but drives “can’t track” criteria) | Yes |
| 4.5 | Grocery store customer (movement) analysis | Out of scope (but drives “can’t track” criteria) | Yes |
| 4.6 | Grocery store frequent shopper | In scope, (assuming we evaluate criteria): | Yes |
| 4.7 | Infrastructure with different SSIDs | Out of scope | Yes |
| 4.8 | Infrastructure use of probes | Perhaps only recommendations in Spec.Anything about address in [directed?] probes to other APs in the same ESS when associated? | Yes |
| 4.9 | Unapproved client detection | Out of scope | Yes |
| 4.10 | Approved client in secured environment | Maps partially to post-association use cases, and partially a pre-association issue? | Yes |
| 4.11 | Approved and secured client taking unexpected actions | Out of scope | Yes |
| 4.12 | Unapproved AP detection | Not an RCM issue; out of scope | Yes |
| 4.13 | Mobile AP | ~~Out of scope~~Might add some recommendations? (But, might consider a solution, if one presented – would need to address the lack of this terminology in 802.11) | Yes |
| 4.14 | Onboarding a “known” MAC address | Can be solved with 802.1X security, or SAE passwords, or Wi-Fi Easy Connect, or BRSKI (where does the list end – out of band anything?)?.Might add recommendations to suggest those solutions? | Yes |
| 4.15 | Customer support and troubleshooting | Aspects are within our scope, might be alternative interface(s) to access and/or control the MAC address behavior. | Yes |
| 4.16 | Residential gateway with public hotspot | Out of scope | Yes |
| 4.17 | Lawful surveillance | Out of scope | Yes |
| 4.18 | Emergency services | Out of scope | Yes |
| 4.19 | Public Wi-Fi hotspot roaming | Out of scope/covered by above use cases | Yes |
| 4.20 | MAC address collisions (WBA) | Out of scopeCould add recommendations on ways to help avoid the problem | Yes |
| 4.21 | Accounting and billing issues (WBA) | Nothing new. Out of scope, Was “a broken idea” (not an appropriate/reliable identifier) in the first place. | Yes |
| 4.22 | QoS and QoE (WBA) | Can be solved with 802.1X security, or SAE passwords, or Wi-Fi Easy Connect, or BRSKI (where does the list end – out of band anything?)?.Might add recommendations to suggest those solutions? | Yes |
| 4.23 | DHCP pool exhaustion | Might add recommendations. | Yes |
| 4.24 | Inconsistent DHCP address assignment (WBA) | At best, recommendations (same recommendations as 4.23?). Really out of scope. | Yes |
| 4.25 | ACLs/firewalls (WBA) | Same as use case 4.2.ORIP-based ACL, is out of scope | Yes |

# Proposed Solutions

## Signature-based method for identifying STAs

[**11-21/1083r0**](https://mentor.ieee.org/802.11/dcn/21/11-21-1083-00-00bh-a-signature-based-method-for-identifying-stas-with-randomized-mac-addresses.pptx)

**[11-21/2039r0](https://mentor.ieee.org/802.11/dcn/21/11-21-2039-00-00bh-random-index-assisted-scheme-for-reducing-rcm-sta-identification-complexity.pptx)**

**[11-22/0054r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0054-00-00bh-signature-based-rcm-sta-identification-solution-analyses.docx)**

## Identifiable random MAC address

[**11-21/1585r9**](https://mentor.ieee.org/802.11/dcn/21/11-21-1585-09-00bh-identifiable-random-mac-address.pptx)

[**11-21/1673r6**](https://mentor.ieee.org/802.11/dcn/21/11-21-1673-06-00bh-proposed-text-for-irma.docx)

[**11-21/1720r1**](https://mentor.ieee.org/802.11/dcn/21/11-21-1720-01-00bh-irm-advantages-and-use-cases.docx)

**[11-21/2006r1](https://mentor.ieee.org/802.11/dcn/21/11-21-2006-01-00bh-irm-analysis-uses-cases-criteria.docx)**

**[11-22/0118r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0118-00-00bh-irma-with-id-query.pptx)**

**[11-22/0085r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0085-00-00bh-irma-and-spoof-discussion.pptx)**

## Client ID query

[**11-21/1378r0**](https://mentor.ieee.org/802.11/dcn/21/11-21-1378-00-00bh-client-id-query-concept.pptx)

[**11-21/1379r3**](https://mentor.ieee.org/802.11/dcn/21/11-21-1379-03-00bh-proposed-text-for-id-query-action-frame.docx)

**[11-21/1853r2](https://mentor.ieee.org/802.11/dcn/21/11-21-1853-02-00bh-id-query-analysis.docx)**

## Transient STA ID

**[11-21/1839r1](https://mentor.ieee.org/802.11/dcn/21/11-21-1839-01-00bh-transient-sta-id.pptx)**

**[11-22/0025r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0025-00-00bh-tsid-analysis.docx)**

## Secure Device ID exchange

**[11-22/0117r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0117-00-00bh-secure-device-id-exchange-concept.pptx)**

## Opaque Device ID

**[11-22/0154r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0154-00-00bh-opaque-device-id.pptx)**

## STA Generated Device ID

**[11-22/0158r3](https://mentor.ieee.org/802.11/dcn/22/11-22-0158-03-00bh-sta-generated-device-id.docx)**

## MAC Address Designation (MAAD)

**[11-22/0157r3](https://mentor.ieee.org/802.11/dcn/22/11-22-0157-03-00bh-mac-address-designation-maad.pptx)**

**[11-22/0301r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0301-00-00bh-maad-mac-text.docx)**

## Network Generated Device ID

**[11-22/0187r1](https://mentor.ieee.org/802.11/dcn/22/11-22-0187-01-00bh-network-generated-device-id.docx)**

## Solutions analysis

The following table summarizes the in-scope use cases (per clause 5), to aid in evaluating each solution’s applicability to those use cases.

**Table 1 – Analysis against Use Cases**

|  |  |  |
| --- | --- | --- |
| Use Case # | Description |  |
| 4.1  | Pre-association client steering.“Nice to have”, if can find sufficient privacy controls (opt-in, etc.) – maybe as a recommendation? Maybe if a solution to another problem happens to solve this? |  |
| 4.2 | Post-association (returning device) device identification.Focus on a “returning device” needing identification on per network/SSID basis. |  |
| 4.3 | Post-association home automation/arrival detection |  |
| 4.6 | Grocery store frequent shopper.(Only in scope if criteria in Table 2 are not compromised.) |  |
| 4.8 | Infrastructure use of probes.Perhaps only recommendations in Spec. |  |
| 4.10 | Approved client in secured environment.Similar to 4.1 and 4.2, for pre-association and post-association situations, respectively. |  |
| 4.13 | Mobile AP.Might add some recommendations? (But, might consider a solution, if one presented – would need to address the lack of this terminology in 802.11) |  |
| 4.15 | Customer support and troubleshooting.Aspects are within our scope, might be alternative interface(s) to access and/or control the MAC address behavior. |  |
| 4.20 | MAC address collisions (WBA raised).Out of scope to resolve. Could add recommendations on ways to help avoid the problem |  |
| 4.23 | DHCP pool exhaustion.Might add recommendations. |  |
| 4.24 | Inconsistent DHCP address assignment (WBA raised).At best, recommendations (same recommendations as 4.23?). Really out of scope. |  |

The following table summarizes features of the in-scope use cases (per clause 5), to aid in evaluating each solution’s applicability to those use features.

**Table 2 – Analysis against features/attributes/criteria**

|  |  |  |
| --- | --- | --- |
|  | Attribute/criteria |  |
| 1 | User opt-in, per network |  |
| 2 | Third-party (attackers/parties not intended to have the identification) can’t track – device can use a different address when returning/over time |  |
| 3 | No exposure of PII that had been hidden by RCM? |  |
| 4 | Network can provide user services (automation, access control, etc.) – device can return to same ESS |  |
| 5 | Network can use for troubleshooting |  |
| 6 | Network can provide QoS, DHCP, services |  |
| 7 | Pre-association client identification is possible (nice-to-have) |  |
| 8 | Is it “Extensible”? (Nice-to-have?) |  |
| 9 | Processing required on AP one-time/infrequent |  |
| 10 | Processing required on AP each association |  |
| 11 | Processing required on non-AP STA one-time/infrequent |  |
| 12 | Processing required on non-AP STA each association |  |
| 13 | Setup complexity for AP administrator |  |
| 14 | Setup complexity to configure non-AP STA |  |
| 15 | Memory/storage requirements on AP (consider large # of clients) |  |
| 16 | Memory/storage requirements on non-AP STA |  |
| 17 | Third-party can determine if non-AP STA is using the solution? |  |
| 18 | Solution depends on an encrypted link? (Nice to have if ‘no’?) |  |
| 19 | How strongly is the ID bound to a user, and giving the user access/capabilities/etc.? |  |
| 20 | Is it important/critical that the AP is trusted? |  |
| 21 | How “real” is the ID, in terms of getting to actual end-user identification versus a throwaway? |  |
| 22 | How much the network can trust the ID, to re-establish context from last time? (Spoofing protection) Level of trust of the ID should match the trust of the data exchange with this network. |  |
| 23 | How does client know level of trust of the network (trust of AP/infrastructure/back-end entities)? |  |
| 24 | Consider operation of the solution on networks that are “Open”, or PSK and could be exposed. (Note that protection of (post-association/SA) identifier is no higher than protection of the data exchange. Not a new problem caused by RCM.) |  |
| 25 | Control over lifetime of the identifier? User control and/or network control? |  |
| 26 | Consider whether solution offers identifier per device, user or group. |  |
| 27 | Network being spoofed can gain access to client identifier? |  |